

What is claimed is:

1 1: A method of generating a Service Ticket for a requested Service comprising:
2 receiving a request,for a Service Ticket from a client;
3 generating a session key;
4 encrypting a cipher text with the session key
5 determining a number of servers designated to provide the requested service;
6 for each providing server, encrypting the session key with a secret key associated
7 with each respective server;
8 creating a Service Ticket that includes an encrypted session key for each
9 providing server, and the encrypted cipher text; and
10 transmitting the Service Ticket to the client.

1 2: The method of claim 1, further including:
2 generating a Ticket-Granting-Ticketing utilizing a protocol substantially in
3 compliance with the Kerberos protocol; and
4 wherein receiving a request for a Service Ticket from a client further includes
5 receiving the Ticket-Granting-Ticket from the client.

1 3: The method of claim 1, wherein determining the number of servers designated to
2 provide the requested service includes:
3 utilizing a database that maps a generic server name to a specific server name; and
4 setting the numbers of servers designated to provide the service equal to the

5 number of specific server names mapped to the generic server name that provides the
6 requested service.

1 4: The method of claim 3, wherein utilizing a database that maps a generic server name
2 to a specific server name includes selecting a database from a group consisting essentially
3 of:

4 a domain name server database,
5 a database associated with a Key Distribution Center, and
6 a Kerberos database.

1 5: The method of claim 3, wherein the secret keys associated with each providing server
2 are not synchronized across the providing servers.

1 6: The method of claim 1, wherein the created Service Ticket includes:
2 a header that designates the Service Ticket as a format that includes multiple
3 encrypted session keys,
4 a field that expressly designates the number of encrypted session keys,
5 an encrypted session key for each providing server, and
6 the encrypted cipher text.

1 7: The method of claim 1, further including:

2 determining if the requested service is provided by a plurality of servers:

3 if not, generating the Service Ticket utilizing a single server mode; and

4 if so, generating the Service Ticket as described in claim 1.

1 8: The method of claim 7, wherein generating the Service Ticket utilizing a single server
2 mode includes:

3 generating a cipher text;

4 encrypting the cipher text with a secret key associated with the providing server;

5 and

6 transmitting the Service Ticket, that includes the encrypted cipher text, to the

7 client.

1 9: A method of authenticating a client's request for a service provided by a service pool
2 comprising;

3 a server receiving a Service Ticket having at least one encrypted session key, and

4 an encrypted cipher text;

5 decrypting the encrypted session key associated with the receiving server utilizing

6 a secret key associated with the receiving server;

7 decrypting the cipher text utilizing the decrypted session key; and

8 providing the service to the client.

1 10: The method of claim 9, wherein receiving a Service Ticket is part of a series of client
2 transactions substantially in compliance with the Kerberos protocol.

1 11: The method of claim 9, wherein decrypting the encrypted session key includes:
2 determining the number of encrypted session keys included within the received
3 Service Ticket;
4 for each encrypted session key, decrypting the encrypted session key utilizing a
5 secret key associated with the receiving server; and
6 wherein decrypting the cipher text utilizing the decrypted session key includes
7 for each encrypted session key, attempting to decrypt the cipher text with the
8 decrypted session key;
9 if the cipher text is successfully decrypted, providing the service to the client.

1 12: The method of claim 9, wherein decrypting the encrypted session key associated
2 with the receiving server utilizing a secret key associated with the receiving server
3 includes:
4 utilizing a server identifier to determine which encrypted session key is associated
5 with the receiving server; and
6 decrypting the associated encrypted session key utilizing a secret key associated
7 with the receiving server.

1 13: The method of claim 9, further including:

2 determining if the received Service Ticket includes a plurality of encrypted

3 session keys for multiple servers

4 if not, processing the ticket in a single server mode; and

5 if so, processing the ticket as described in claim 9.

1 14. The method of claim 13, wherein processing the ticket in a single server mode

2 includes processing the Service Ticket in utilizing a process substantially compliant with

3 the Kerberos protocol.

1 15. The method of claim 9, wherein receiving a Service Ticket includes:

2 a managing agent receiving a Service Ticket;

3 the managing agent selecting a receiving server from a server pool having a

4 plurality of servers;

5 routing the Service Ticket to the receiving server.

1 16. The method of claim 15, wherein the plurality of servers each include a secret key

2 associated with the respective servers, and the plurality of secret keys are not

3 synchronized among the plurality of servers..

1 17. The method of claim 16, wherein the server pool functions as a group of independent
2 computers working together as a single system.

1 18. A Key Distribution Center comprising:
2 an Authentication Service that is capable of
3 authenticating that a client may legitimately access the Key Distribution
4 Center, and
5 issuing a Ticket-Granting-Ticket to the client; and
6 a Ticket Granting Service that is capable of
7 accepting the Ticket-Granting-Ticket from the client, and
8 issuing a Multi-Server Service Ticket to the client; and
9 wherein the Multi-Server Service Ticket allows the client access a network
10 service that is provided by a plurality of servers.

1 19. The Center of claim 18, wherein the Multi-Server Service Ticket includes:
2 encrypted session keys for each of the respective plurality of servers, and an
3 encrypted cipher text;
4 wherein, there is only one plaintext session key, each encrypted session key is formed by
5 encrypting the plaintext session key with a secret key associated with a respective server

6 of the plurality of servers, and the encrypted cipher text is encrypted with the plaintext
7 session key.

1 20. The Center of claim 18, wherein Authentication Server is capable of
2 authenticating that a client may legitimately access the Key Distribution Center, and
3 issuing a Ticket-Granting-Ticket to the client,
4 utilizing a protocol substantially in compliance with the Kerberos protocol.

1 21. The Center of claim 19, wherein the Ticket Granting Service is capable of issuing a
2 Multi-Server Service Ticket to the client and further includes the capability to:
3 generating a session key;
4 encrypting a cipher text with the session key
5 determining the number of servers designated to provide the requested service;
6 for each providing server, encrypting the session key with a secret key associated
7 with each respective server;
8 creating a Multi-Server Service Ticket that includes an encrypted session key for
9 each providing server, and the encrypted cipher text; and
10 transmitting the Multi-Server Service Ticket to the client.

1 22. The Center of claim 21, wherein the Ticket Granting Service capability to determine
2 the number of servers designated to provide the requested service includes:

3 utilizing a database that maps a generic server name to a specific server name; and
 4 setting the numbers of servers designated to provide the service equal to the
 5 number of specific server names mapped to the generic server name that provides the
 6 requested service.

1 23. The Center of claim 22, wherein Ticket Granting Service capability of utilizing a
 2 database that maps a generic server name to a specific server name includes selecting a
 3 database from a group consisting essentially of:
 4 a domain name server database,
 5 a database associated with a Key Distribution Center, and
 6 a Kerberos database.

1 24. A system comprising:
 2 a Key Distribution Center having:
 3 an Authentication Service that is capable of
 4 authenticating that a client may legitimately access the Key
 5 Distribution Center, and
 6 issuing a Ticket-Granting-Ticket to the client; and
 7 a Ticket Granting Service that is capable of
 8 accepting the Ticket-Granting-Ticket from the client, and
 9 issuing a Multi-Server Service Ticket to the client;
 10 a plurality of servers that are each capable of providing the client with a network

11 service; and
12 wherein the Multi-Server Service Ticket allows the client access the network
13 service provided by the plurality of servers.

1 25. The system of claim 24, wherein the Multi-Server Service Ticket includes:
2 encrypted session keys for each of the respective plurality of servers, and an
3 encrypted cipher text;
4 wherein, there is only one plaintext session key, each encrypted session key is formed by
5 encrypting the plaintext session key with a secret key associated with a respective server
6 of the plurality of servers, and the encrypted cipher text is encrypted with the plaintext
7 session key.

1 26. The system of claim 24, wherein Authentication Server is capable of utilizing a
2 protocol substantially in compliance with the Kerberos protocol.

1 27. The system of claim 26, wherein the Ticket Granting Service is capable of issuing a
2 Multi-Server Service Ticket to the client and further includes the capability to:
3 generating a session key;
4 encrypting a cipher text with the session key
5 determining the number of servers designated to provide the requested service;
6 for each providing server, encrypting the session key with a secret key associated

7 with each respective server;
8 creating a Multi-Server Service Ticket that includes an encrypted session key for
9 each providing server, and the encrypted cipher text; and
10 transmitting the Multi-Server Service Ticket to the client.

1 28. The system of claim 27, wherein the Ticket Granting Service capability to determine
2 the number of servers designated to provide the requested service includes:
3 utilizing a database that maps a generic server name to a specific server name; and
4 setting the numbers of servers designated to provide the service equal to the
5 number of specific server names mapped to the generic server name that provides the
6 requested service.

1 29. The system of claim 28, wherein Ticket Granting Service capability of utilizing a
2 database that maps a generic server name to a specific server name includes selecting a
3 database from a group consisting essentially of:
4 a domain name server database,
5 a database associated with a Key Distribution Center, and
6 a Kerberos database.

1 30. The system of claim 27, wherein the plurality of servers is capable of authenticating a
2 client's request for a service utilizing;

3 receiving a Multi-Server Service Ticket having at least one encrypted session key,
 4 and an encrypted cipher text;
 5 assigning a receiving server from among the plurality of servers to service the
 6 Service request;
 7 decrypting the encrypted session key associated with the receiving server utilizing
 8 a secret key associated with the receiving server;
 9 decrypting the cipher text utilizing the decrypted session key; and
 10 utilizing the receiving server to provide the service to the client.

1 31: The system of claim 30, wherein each server of the plurality of servers is capable of
 2 being the receiving server and the receiving server is capable of:
 3 decrypting the encrypted session key associated with the receiving server utilizing
 4 a secret key associated with the receiving server;
 5 decrypting the cipher text utilizing the decrypted session key; and
 6 providing the service to the client.

1 32: The system of claim 31, wherein decrypting the encrypted session key includes:
 2 determining the number of encrypted session keys included within the received
 3 Multi-Server Service Ticket;
 4 for each encrypted session key, decrypting the encrypted session key utilizing a
 5 secret key associated with the receiving server; and
 6 wherein decrypting the cipher text utilizing the decrypted session key includes

7 for each encrypted session key, attempting to decrypt the cipher text with the
8 decrypted session key;
9 if the cipher text is successfully decrypted, providing the service to the client.

1 33: The system of claim 30, wherein plurality of servers are configured as a cluster and
2 are capable of functioning as a group of independent computers that work together as a
3 single system.

1 34: An article comprising:
2 a storage medium having a plurality of machine accessible instructions, wherein when the
3 instructions are executed, the instructions provide for:
4 receiving a request for a Service Ticket from a client;
5 generating a session key;
6 encrypting a cipher text with the session key
7 determining the number of servers designated to provide the requested service;
8 for each providing server, encrypting the session key with a secret key associated
9 with each respective server;
10 creating a Service Ticket that includes an encrypted session key for each
11 providing server, and the encrypted cipher text; and
12 transmitting the Service Ticket to the client.

1 35: The article of claim 34, further including instructions providing for:
2 generating a Ticket-Granting-Ticketing utilizing a protocol substantially in
3 compliance with the Kerberos protocol; and
4 wherein receiving a request for a Service Ticket from a client further includes
5 receiving the Ticket-Granting-Ticket from the client.

1 36: The article of claim 34, wherein the instructions providing for determining the
2 number of servers designated to provide the requested service includes instructions
3 providing for:
4 utilizing a database that maps a generic server name to a specific server name; and
5 setting the numbers of servers designated to provide the service equal to the
6 number of specific server names mapped to the generic server name that provides the
7 requested service.

1 37: The article of claim 36, wherein the instructions providing for utilizing a database
2 that maps a generic server name to a specific server name includes instructions providing
3 for selecting a database from a group consisting essentially of:
4 a domain name server database,
5 a database associated with a Key Distribution Center, and
6 a Kerberos database.

1 38: The article of claim 36, wherein the secret keys associated with each providing
2 server are not synchronized across the providing servers.

1 39: The article of claim 38, wherein the instructions providing for creating a Service
2 Ticket further includes instructions providing for creating a Service Ticket that includes:
3 a header that designates the Service Ticket as a format that includes multiple
4 encrypted session keys,
5 a field that expressly designates the number of encrypted session keys,
6 an encrypted session key for each providing server, and
7 the encrypted cipher text.

1 40: The article of claim 34, further including instructions providing for:
2 determining if the requested service is provided by a plurality of servers:
3 if not, generating the Service Ticket utilizing a single server mode; and
4 if so, generating the Service Ticket as described in claim 1.

1 41: The article of claim 40, wherein the instructions providing for generating the Service
2 Ticket utilizing a single server mode includes instructions providing for:
3 generating a cipher text;
4 encrypting the cipher text with a secret key associated with the providing server;
5 and

6 transmitting the Service Ticket, that includes the encrypted cipher text, to the
7 client.

1 42: An article comprising:

2 a storage medium having a plurality of machine accessible instructions, wherein when the
3 instructions are executed, the instructions provide for:

4 a server receiving a Service Ticket having at least one encrypted session key, and
5 an encrypted cipher text;

6 decrypting the encrypted session key associated with the receiving server utilizing
7 a secret key associated with the receiving server;

8 decrypting the cipher text utilizing the decrypted session key; and

9 providing the service to the client.

1 43: The article of claim 42, wherein the instructions provide for receiving a Service
2 Ticket are part of a series of client transactions substantially in compliance with the
3 Kerberos protocol.

1 44: The article of claim 42, wherein the instructions provide for decrypting the encrypted
2 session key includes instructions provide for:

3 determining the number of encrypted session keys included within the received
4 Service Ticket;

5 for each encrypted session key, decrypting the encrypted session key utilizing a
6 secret key associated with the receiving server; and
7 wherein decrypting the cipher text utilizing the decrypted session key includes
8 for each encrypted session key, attempting to decrypt the cipher text with the
9 decrypted session key;
10 if the cipher text is successfully decrypted, providing the service to the client.

1 45: The article of claim 42, wherein the instructions provide for decrypting the encrypted
2 session key associated with the receiving server utilizing a secret key associated with the
3 receiving server includes instructions provide for:

4 utilizing a server identifier to determine which encrypted session key is associated
5 with the receiving server; and
6 decrypting the associated encrypted session key utilizing a secret key associated
7 with the receiving server.

1 46: The article of claim 42, further including instructions provide for:

2 determining if the received Service Ticket includes a plurality of encrypted
3 session keys for multiple servers
4 if not, processing the ticket in a single server mode; and
5 if so, processing the ticket as described in claim 9.

1 47. The article of claim 46, wherein the instructions provide for processing the ticket in a
2 single server mode includes instructions provide for processing the Service Ticket in
3 utilizing a process substantially compliant with the Kerberos protocol.

1 48. The article of claim 42, wherein the instructions provide for receiving a Service
2 Ticket includes instructions provide for:
3 a managing agent receiving a Service Ticket;
4 the managing agent selecting a receiving server from a server pool having a
5 plurality of servers;
6 routing the Service Ticket to the receiving server.

1 49. The article of claim 48, wherein the plurality of servers each include a secret key
2 associated with the respective servers, and the plurality of secret keys are not
3 synchronized among the plurality of servers..

1 50. The article of claim 49, wherein the server pool functions as a group of independent
2 computers working together as a single system.